学校编码：10384
学号：X2011230205
分类号_____密级_____
UDC_

工 程 硕 士 学 位 论 文

基于虚拟技术的党政机关计算机安全环境构建研究与应用

Research and Application of Computer Security Environment Construction for Party and Government Organizations Based on Virtualization Technology

周志远

指 导 教 师：龙 飞 副 教 授
专 业 名 称：软 件 工 程
论文提交日期：2013 年 4 月
论文答辩日期：2013 年 5 月
学位授予日期：2013 年 月

指 导 教 师：_____
答辩委员会主席：_____

2013 年 4 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　√　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘　要

国家党政机关涉密部门由于所担负工作任务的特殊性，需要健全的计算机安全环境，以保证数据存储安全和避免工作信息非法外泄。要做到这一点，既要从制度、教育、培训等方面加大管理力度，更要从技术上提供保障手段。传统的计算机安全技术难以进行用户管理控制，用其构建的计算机环境存在诸多无法克服的安全隐患，本文通过对基于 x86 体系结构的虚拟化技术的应用研究，实现国家党政机关计算机安全环境的构建。

在传统的计算机环境中，用户与计算机之间在物理上没有隔离，每位用户既是计算机的使用者，又是计算机的管理者，这导致了机关涉密要害部门的计算机环境存在以下安全隐患：实现了内网与外网的隔离，但是一机两用、一机双网的现象屡禁不止；计算机分散使用、分散管理，使别有用心的人有机可乘；缺乏专门的数据备份和恢复设备，存在数据损坏和丢失的风险；安全保密软件不能实现强制安装，很容易被卸载或通过重装操作系统进行清除；用户安装使用软件随意性较大，容易在网络中种植木马程序或造成病毒蔓延；计算机数据传输接口和输入输出设备不易控制，造成敏感数据非法外泄。

本文从计算机安全角度出发，针对国家党政机关涉密部门中的上述计算机安全隐患，通过实验对虚拟化技术进行功能验证，通过实例对计算机安全环境进行构建仿真。实验和仿真结果表明，虚拟化技术可以从物理基础架构就开始对计算机提供全方位的安全保护，具有传统计算机安全技术无法比拟的优势，通过运用虚拟化技术，可以实现将用户的角色仅仅定 位于计算机的使用者，不仅解决了用户管理难题，而且实现了全方位的数据保护，从而消除目前涉密部门中潜在的各类计算机安全隐患，为构建安全可靠的计算机工作环境奠定了坚实基础。

关键词：计算机安全；虚拟技术；用户管理

Abstract

The special nature of the tasks assumed by the departments concerning security in national party and government organizations demands a sound and secure computer environment, which ensures data storage security and guards against the illegal leakage of work information. In order to achieve this end, the management of institution, education and training needs to be strengthened, and more importantly, necessary technical support is required. Traditional computer security technology has difficulty in user management, and the computer environment thus built poses many security risks that can not be overcome. With application research on the x86 architecture based virtualization technology, this paper aims at the construction of computer security environment for national party and government organizations.

In the traditional computer environment, the user and the computer are not physically isolated; therefore, each user is both a computer user and a computer administrator. This leads to the following security risks in the computer environment of the departments concerning security in national party and government organizations: although there is isolation between internal and external networks, there are repeated violations of bans on the practice of one computer for both agency work and personal use, and that of one computer with dual- network; personnel with ulterior motives can take advantage of scattered and unorganized computer use and management; the lack of special equipment for data backup and recovery may lead to data corruption and loss; the installation of the security software for can not be guaranteed; thus the security software is easy to be uninstalled or removed through reinstallation of the operating system; users' casual installation and use of software lead to the easy planting of Trojan or the wide spread of viruses in the network; computer data transmission interfaces and the I/O devices are hard to control, resulting in the illegal leakage of sensitive data.

From the perspective of computer security, and the potential computer security risks in the departments concerning security in national party and government organizations in particular, this paper conducted functional verification experiments on virtualization technology, and carried out simulation construction of computer security environment based on concrete examples. Experimental and simulation

results show that virtualization technology can provide a physical infrastructure for a full range of computer security, which the traditional computer security techniques can not match at all. Through the use of virtualization technology, the user's role can be assigned as computer user only, and this can not only solve the problem of user management, but also achieve a full range of data protection. Consequently, various types of potential computer security risks in the current departments concerning security can be eliminated; hence a solid foundation for a secure and reliable computer environment can be laid.

Key Words: Computer Security; Virtualization; User Management

目 录

Contents

第一章 绪论

1.1. 研究背景及意义

随着人类社会进入信息时代，计算机成为信息存储和传播的主要载体。计算机在为工作和生活提供便利的同时，也存在诸多安全问题。我国党政机关涉密部门的计算机安全环境总体上是好的，但也存在敏感信息的失密、泄密、窃密等现象。这些安全问题的产生，有的是由于技术保障措施不足造成的，如硬盘损坏而造成信息的不完整或不可用；有的是由于管理方面出现的问题，如非核心涉密人员接触涉密计算机、涉密计算机接入互联网、涉密载体在办公计算机和个人计算机之间混用；还有的是由于个别人思想存在误区，保密意识不强甚至主动出卖涉密信息。项目开发背景及意义。

当前，我国党政机关针对涉密计算机的使用制定了较为完备的规范、法规，也推广了一些安全保密软件，这些措施对于构建计算机安全环境起到了积极作用。同时，由于政务网采用的是独立的专网，也在一定程度上提高了安全性。但是，办公计算机和使用这些计算机的用户数量众多，分布广泛，导致这些规范、法规不能够被全部执行，安全保密软件也不能保证安装到每一台办公计算机上，并且这些规范、法规和安全保密软件对用户使用计算机带来一些限制，会导致一些用户将这些安全措施视作绊脚石而规避使用。政务网由于地域广，使用单位分散，也带来了一些不安全因素，在网络环境中，由于 TCP/IP协议在设计之初更关注网络的联通和高效率，未重视安全问题，导致协议中存在很多安全漏洞或隐患。硬件、软件的具体实现或系统安全策略上存在的漏洞也给计算机安全带来巨大威胁[1]。

网络环境中的计算机不再是孤立的个体，每一台计算机都可能成为安全隐患点，这样的隐患点会辐射并影响大范围的联网计算机。别有用心的人可以借助某台计算机入侵网络中的其它计算机，或者使用计算机临时加入内部网络实施入侵活。为了保密工作需要，涉密部门要求连接互联网的计算机要与内部网计算机物理隔离，但“一机双网”的现象仍时有发生。只要出现这样的隐患点，整个涉密机关内网的计算机都处于安全威胁当中。党政机关中的重要涉密部门出于安全方面

的考虑，不允许涉密计算机连接外网，出于对“网络猛于虎”的忌惮，甚至不允许建立内部局域网。即使这样，失泄密案件仍时有发生，因为还存在着“一机两用”的 现象，出于有意或是无意，办公计算机成为了个人计算机，被用来连接互联网。

“一机双网”和“一机两用”都跟互联网有关。互联网本来是先进的事物，但在安全保密工作面前却变成了吃人的猛虎。随着信息技术的发展，接入互联网变得非常容易，除了通过电话线路，现今的智能手机、3G 手机通过在计算机上安装相应的程序，也可以方便地把计算机连接上互联网。由于涉密计算机数量众多，分布广泛，对计算机的安全管控变得非常困难，党政机关的安全保密部门整日疲于“堵漏”和“扑火”。涉密部门每次组织对系统内的计算机进行安全排查，需要投入大量的 人力、物力，排查周期长，虽然可以取得一定的效果，但不能从根本上杜绝计算机失泄密案件的发生。每次发生失泄密案件之后，又要在有关部门进行通报批评、教育整顿，不但影响正常的工作安排，也未能从根本上阻止个别人重蹈覆辙。党政机关在不断加强计算机安全水平的同时也加重了管理的负担和降低了计算机的易用性。在一些重要涉密部门，所有计算机都处于单机工作状态，平时需要共享资料时，就用光盘进行刻录，将资料从一台计算机转移到另一台计算机。这种方式费时费力，降低工作效率，也不能从根本上满足安全保密需要。只要有人另有所图，通过计算机上自带的刻录光驱或者打印机同样可以将涉密资料拷贝或者打印出来。

计算机失泄密案件是血淋淋的，是触目惊心的，是令人痛心疾首的，不但极大地影响了党政机关涉密部门的形象和声誉，给国家建设带来巨大损失，甚至还影响了国家安全。在这些案例当中，除了极少数人，大部分人是出于“无意”或者“无知”而造成失泄密事件的发生，这些人从某种意义上讲是属于“好人”的，并不是站在我们对面立场的敌对分子。如果我们在技术手段上提供更为健全的计算机安全保护措施，不仅可以减少由于失泄密问题带来的严重损失，也能更大程度地保护我们自己的同志。

虚拟化技术可以实现计算机的集中管理，并通过制定策略强制执行 安全措施，为解决传统计算机环境下的安全问题提供了较好的方案，虚 拟化技术还可以在加强计算机安全水平的同时提高计算机的方便易用性。构建党政机关涉密部门计算机安全环境是十分重要和迫切的现实需要，正是在这样的背景之下，本文